500-285^{Q&As}

500-285^{Q&As}

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Pass Cisco 500-285 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/500-285.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Suppose an administrator is configuring an IPS policy and attempts to enable intrusion rules that require the operation of the TCP stream preprocessor, but the TCP stream preprocessor is turned off. Which statement is true in this situation?

A. The administrator can save the IPS policy with the TCP stream preprocessor turned off, but the rules requiring its operation will not function properly.

B. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the TCP stream preprocessor will be turned on for the IPS policy.

C. The administrator will be prevented from changing the rule state of the rules that require the TCP stream preprocessor until the TCP stream preprocessor is enabled.

D. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the rules that require the TCP stream preprocessor will be turned off for the IPS policy.

Correct Answer: B

QUESTION 2

Which statement represents detection capabilities of the HTTP preprocessor?

A. You can configure it to blacklist known bad web servers.

B. You can configure it to normalize cookies in HTTP headers.

C. You can configure it to normalize image content types.

D. You can configure it to whitelist specific servers.

Correct Answer: B

QUESTION 3

What does packet latency thresholding measure?

A. the total elapsed time it takes to process a packet

B. the amount of time it takes for a rule to process

C. the amount of time it takes to process an event

D. the time span between a triggered event and when the packet is dropped

Correct Answer: A

QUESTION 4

A user discovery agent can be installed on which platform?

A. OpenLDAP

B. Windows

C. RADIUS

D. Ubuntu

Correct Answer: B Testlet 1

TESTLET OVERVIEW

Title: Case Study

The following testlet will present a Case Study followed by [count] multiple choice question(s), [count]

create a tree question(s), [count] build list and reorder question(s) and [count] drop and connect question

(s).

You will have [count] minutes to complete the testlet.

For help on how to answer the questions, click the Instuctions button on the question screen.

QUESTION 5

Which feature of the preprocessor configuration pages lets you quickly jump to a list of the rules associated with the preprocessor that you are configuring?

A. the rule group accordion

B. a filter bar

C. a link below the preprocessor heading

D. a button next to each preprocessor option that has a corresponding rule

Correct Answer: C